ORIGINAL

EX PARTE OR LATE FILED

AT&T

295 North Maple Avenue
Basking Ridge, NJ 07920

December 1, 1994

RECEIVED

DEC 1 1994

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF SECRETARY

William F. Caton
Acting Secretary
Federal Communications Commission
1919 M. Street, N.W. - Room 222
Washington, DC 20554

Re: Ex Parte Presentation
CC Docket No.: 93-292 - Toll Fraud

Dear Mr. Caton:

Today, Peter Coulter of AT&T, Marie Breslin and Mary Chacanias both of Bell Atlantic and I met with Linda Dubroof and Pam Gerr of the FCC Domestic Facilities Division to discuss several recent well publicized incidents of Toll Fraud; their root causes, existing methods for detecting toll fraud and possible solutions for minimizing or eliminating this type of toll fraud in the future. The attached documents were used to facilitate the discussion.

Two copies of this Notice were submitted to the Secretary of the FCC in accordance with Section 1.1206(a)(1) of the Commission's Rules.

Sincerely,

Frank Simone
District Manger
Federal Government Affairs

Attachments

cc: M. Breslin
M. Chacanias
P. Coulter
L. Dubroof
P. Gerr

No. of Copies rec'd 0+1
List A B C D E

Huge Calling-Card Scheme Uncovered

International Ring Sold Account Numbers Stolen From Computer Files

By Bill Miller
Washington Post Staff Writer

An international ring of computer hackers gained access to thousands of telephone calling card numbers that were used to make at least $1.5 million in long-distance calls, federal authorities said yesterday.

Federal officials said the case could become one of the biggest telecommunications fraud schemes ever uncovered. Only a small fraction of the losses have been totaled in the two-month investigation, they said.

Authorities said the ring's members sold account numbers pilfered from a long-distance carrier based in the District to people throughout the United States and Europe, who then racked up enormous long-distance charges.

"These hackers-turned-con artists were using computers to pass along the calling card numbers," said David Adams, a spokesman for the Secret Service. "They were making very handsome illegitimate salaries on this."

All told, the group obtained at least 40,000 calling card numbers issued by AT&T Corp., GTE Corp., MCI Communications Inc. and other major companies. The telephone companies covered the losses after customers called to complain of huge monthly bills.

The ring's alleged leader—who lived on an island off the coast of Spain—was arrested after authorities tape-recorded his boasts that he was making more than $18,000 a month on the scheme, prosecutors said.

Max Louarn, 22, was ordered held without bond after a hearing yesterday at U.S. District Court in Alexandria.

Louarn, a native of France, has homes in Spain, France and Germany, and numerous overseas bank accounts, said Assistant U.S. Attorney John N. Nassikas III.

Louarn was arrested when he flew to Dulles International Airport on Sept. 20 to meet with one of his alleged accomplices—a Woodbridge man who provided most of the numbers. That man, Andy Gaspard, 23, agreed to cooperate with the Secret Service after a search of his home turned up evidence of his involvement in the scheme, investigators said.

Gaspard, who has not been charged, worked for Cleartel Communications, a long-distance operator service based in the District. Cleartel keeps track of calling-cards used on its service.

According to court documents, Gaspard has told investigators that he began selling the numbers in 1992, the year he started work for Cleartel. He recorded the numbers at work and then used his personal computer at home to ship them to a man in England, the court papers said.

The Englishman, identified in court documents as Omar Flatekval, 20, has been questioned by authorities in London but no charges have been filed. Prosecutors said Flatekval then used his computer to transmit the numbers to Louarn in Spain.

After he began cooperating with authorities in August, Gaspard left Cleartel. Company officials said yesterday that they had no knowledge of Gaspard's activities and declined to discuss the case.

With Gaspard's help, federal agents tape-recorded numerous telephone calls in recent weeks during which he discussed plans with Flatekval and Louarn, authorities said. Gaspard could not be located for comment yesterday and his attorney did not return a telephone message. James Clark, who represents Louarn, also did not return a message left at his office.

Washington Post 10/27/94

Ringleader Pleads Guilty In Phone Fraud

Calling Card Numbers Were Stolen and Sold

By Bill Miller
Washington Post Staff Writer

A leader of an international ring of computer hackers pleaded guilty yesterday to stealing thousands of telephone calling card numbers that were used to rack up to $140 million in unauthorized long-distance calls.

Max Louarn, of Majorca, Spain, helped orchestrate one of the largest and most sophisticated telephone calling card frauds ever, authorities said. One of his associates described him as "the biggest seller of calling cards in the world," according to court documents filed by prosecutors.

Louarn, 22, was arrested last month after federal agents enlisted the aid of an accomplice to lure him to Northern Virginia. He appeared yesterday in U.S. District Court in Alexandria and pleaded guilty to charges of conspiracy and wire fraud.

Authorities estimated that as many as 140,000 calling card numbers were stolen by a network of thieves operating in the United States, England and Spain. The numbers were issued by carriers such as AT&T Corp., GTE Corp., Bell Atlantic and MCI Communications Inc.

Telephone company officials have estimated that an average of $1,000 in unauthorized charges were made on each of the stolen card numbers.

"Louarn was the major player in the European scheme," said David Adams, a spokesman for the Secret Service, which investigated the case. The numbers were stolen in the United States and then sold in Europe, Adams said.

Authorities said Louarn and others mastered computer software and took advantage of methods used by the telephone companies to keep track of calling card numbers punched in by customers making long-distance calls.

Louarn obtained the pilfered numbers from a network of suppliers in the United States, including some who worked for the telephone companies, authorities said. They said the telephone workers tapped into company computers and devised a way to quickly transmit the numbers to Europe via computer bulletin boards.

Ringleaders sold each number to as many as 20 unauthorized users, according to the court documents filed by Assistant U.S. Attorney John N. Nassikas III.

In the Washington area, Louarn dealt with 23-year-old Andy Gaspard, a former technician for Clear-tel Communications, a long-distance operator service based in the District. Gaspard pleaded guilty this month to a conspiracy charge. Authorities say he provided Louarn's ring with roughly 40,000 calling card numbers.

Gaspard, of Woodbridge, helped lure Louarn to the area last month, supposedly for a visit to arrange a huge turnover of card numbers. Secret Service agents said they followed Gaspard and Louarn to Herndon on Sept. 20 and videotaped a conversation in which Louarn claimed to be making $15,000 a month on the scheme. Then they arrested him.

Gaspard could face up to five years in prison and a fine of $250,000 when he is sentenced Dec. 16. Louarn could face a 10-year prison term and a fine of $250,000 when he is sentenced Jan. 20.

As part of his plea, Louarn said he bought calling card numbers from Ivy James Lay, a technician who worked for MCI at a switching facility in Greensboro, N.C. Lay, who was arrested last month, is accused of stealing as many as 100,000 card numbers. Louarn said he worked with Lay both directly and through intermediaries in California.

419-779-1085

U.S. Department of Justice

United States Attorney

Eastern District of Virginia

1101 King Street
Suite 503
Alexandria, Virginia 22314

703/706-3700
FTS/703-706-3700

PRESS RELEASE

FOR IMMEDIATE RELEASE
SEPTEMBER 29, 1994
ALEXANDRIA, VIRGINIA

HELEN F. FAHEY, UNITED STATES ATTORNEY FOR THE EASTERN DISTRICT OF VIRGINIA, ANNOUNCED THE ARREST TODAY OF MAX LOUARN, AGE 22, OF PALMA DE MALLORCA, SPAIN. LOUARN WAS CHARGED WITH CONSPIRING WITH OTHER PERSONS TO OBTAIN AND USE THOUSANDS OF TELEPHONE CALLING CARD ACCOUNT NUMBERS.

IT IS ALLEGED THAT FROM MAY THROUGH AUGUST OF THIS YEAR LOUARN AND TWO ACCOMPLICES ANDY GASPARD, AGE 23 OF WOODBRIDGE, VIRGINIA AND OMAR FLATEKVAL, AGE 20, OF NORTHUMBRIA, ENGLAND ILLEGALLY OBTAINED TELEPHONE CALLING CARD ACCOUNT NUMBERS.

ACCORDING TO COURT DOCUMENTS, IN AUGUST 1994 THE UNITED STATES SECRET SERVICE BEGAN AN INVESTIGATION REGARDING THE THEFT, DISTRIBUTION, AND FRAUDULENT USE OF AMERICAN TELEPHONE CALLING CARD ACCOUNT NUMBERS THROUGH AN ELECTRONIC COMPUTER BULLETIN BOARD SYSTEM LOCATED IN EUROPE AND THE UNITED STATES. THE SECRET SERVICE, WORKING WITH INVESTIGATORS FROM AT&T, GTE, AND

BELL ATLANTIC, HAS DETERMINED THAT THE THREE CONSPIRATORS MAY BE RESPONSIBLE FOR UNAUTHORIZED USE OF APPROXIMATELY 40,000 CALLING CARDS. INVESTIGATION OF 4,000 OF THESE CARDS HAS SHOWN UNAUTHORIZED CHARGES IN EXCESS OF $1.5 MILLION.

THIS CHARGE OF CONSPIRACY CARRIES A MAXIMUM PENALTY OF 5 YEARS IN PRISON AND A $250,000 FINE.

A PRELIMINARY AND DETENTION HEARING WAS HELD TODAY AND THE DEFENDANT REMAINS IN CUSTODY.

THIS CASE IS BEING INVESTIGATED BY UNITED STATES SECRET SERVICE.

ASSISTANT UNITED STATES ATTORNEY JOHN N. NASSIKAS III IS HANDLING THIS CASE FOR THE UNITED STATES ATTORNEY'S OFFICE.

FURTHER QUESTIONS MAYBE DIRECTED TO THE U.S. ATTORNEY'S OFFICE AND THE UNITED STATES SECRET SERVICE, WASHINGTON FIELD OFFFICE AT 202-435-5100.

####

NOF

Network
Operations Forum

Sponsored by the
Alliance for Telecommunications
Industry Solutions

Date

Mr./Ms. Name
Title
Co
Add
City, State Zip

Dear Mr./Ms.Name:

The Toll Fraud Prevention Committee (TFPC) is a working committee of the Network Operations Forum (NOF), consisting of local exchange carriers, interexchange carriers, and other telecommunication industry participants. Recently, the TFPC addressed the vulnerability and integrity of billing data (commercial credit card and telephone calling card numbers) retained in Aggregator Call Recording Equipment (private pay phones, hotel/motel equipment, etc).

The fraudulent use of calling cards is of great concern to the telecommunications industry. Telephone calling cards are made available expressly for the convenient billing of calls. Tariff restrictions often govern the use of the information obtained by validation customers. Local telephone companies strictly prohibit these customers from retaining calling card data for any purpose other than the validation of billing authorization.

Discussions with manufacturers of private payphones and hotel/motel call recording equipment have indicated that this equipment in many cases by design retains the calling card number and the personal identification numbers (PINs). In some cases this information is still retained after such data is transmitted for validation and billing purposes. Data stored in the call detail record files of private payphone and hotel/motel call recording equipment may also be available to equipment owners and technicians.

To provide some assurance that this information will not be compromised, some equipment manufacturers have enhanced security by encrypting billing records and requiring special modems. However, several manufacturers are not encrypting records and allow the use of standard modems to retrieve billing records. Therefore, if the modem should be accessed by a "hacker", the calling card information and PIN can be obtained without consent. Even with the encryption of billing data, there is little assurance of security, and the improper retention of this data is now suspected of leading to a significant amount of toll fraud.

Rick Harrison, Moderator • Sally N. Katz, Secretary
290 W. Mt. Pleasant Avenue • Room 4E231 • Livingston, NJ 07039
Phone 201 740-3558 • FAX 201 740-6929

Unfortunately, the techniques used by hackers to access and download billing information tored in private pay phones are now published in detail and made widely available in the underground press. In addition, retention of call detail record files creates the opportunity for internal compromise. The TFPC recommends that aggregators that use store and forward technology for alternately billed calls should use pre-call validation to prevent toll fraud, and should not record or retain PINs. Pre-call validation eliminates the necessity to retain PINs in call detail records.

Aggregators utilizing equipment which retains calling card PINs beyond the validation function should contact their telecommunications equipment manufacturer to secure upgrades which will eliminate the need to retain calling card PIN data, and thereby minimize the potential for the abuse that is now growing in the private payphone and hotel/motel markets.

The TFPC also recommends that all manufacturers of payphone equipment and hotel/motel call processing equipment modify the hardware and software of existing equipment and on future versions to eliminate the capability to retain calling card PINs after validation has been completed.

Changes to the North American Numbering Plan in 1995 offer a convenient opportunity for manufacturers to accomplish this task, even for the embedded base of installed payphones. It is also appropriate to improve the capabilities of payphones modems to withstand attacks by hackers, who are often technically proficient and persistent. Other opportunities for fraud (e.g., reprogramming the station for free calls or access to 10XXX1+ or 10XXX011+) present themselves to hackers who have gained unauthorized access to a payphone's internal controls. Therefore, vendors and manufacturers should proactively develop and implement the capabilities required in their products and services to thwart such illegal activities.

If you have any questions, or require additional information, please call me.

Richard P. Harrison
NOF Moderator